What is claimed is:

1. A particular plaintext detector for detecting whether plaintext to be inputted into a predetermined encryption algorithm satisfies a predetermined condition, the particular plaintext detector comprising:

a receiving part for receiving the plaintext;

a counter part for separating a predetermined part from a bit string forming the plaintext into a fixed part and a remaining part into a variable part, counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of the fixed parts, and storing it as a separate count; and

a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number.

2. A particular plaintext detector for detecting whether plaintext to be inputted into a block encryption algorithm satisfies a predetermined condition, the block encryption algorithm receiving and stirring plaintext with a key step by step to perform encryption and outputting ciphertext, the particular plaintext detector comprising:

a receiving part for receiving the plaintext;

a counter part for separating a predetermined part from a bit string forming the plaintext into a fixed part and a remaining part into a variable part, counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of the fixed parts, and storing it as a separate count; and

detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number.

3. A particular plaintext detector for detecting whether plaintext to be inputted into a KASUMI type encryption algorithm having a stirring step satisfies a predetermined condition, the KASUMI type encryption algorithm equal to KASUMI which is a block encryption algorithm that receives plaintext, has a plurality of stirring steps for stir with a key, and performs encryption step by step to output ciphertext, the particular plaintext detector comprising:

a receiving part for receiving the plaintext;

a counter part for separating 17th to 32nd bits of the plaintext from the plaintext into a fixed part and first to 16th bits and 33rd to 64th bits thereof into a variable part, counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts formed of

1 or a plurality of the values of the fixed parts at every set of the values of the fixed parts, and storing it as a separate count; and

a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number.

4. A filter apparatus for limiting output of ciphertext from an encryption algorithm that receives plaintext to output ciphertext, the filter apparatus comprising:

a receiving part for receiving the plaintext;

a counter part for separating a predetermined part from a bit string forming the plaintext into a fixed part and a remaining part into a variable part, counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of the fixed parts, and storing it as a separate count;

a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number; and

a filter apparatus main body for outputting the plaintext when a detection signal is not outputted from the detecting part, and for holding output of the plaintext until it receives a process restart signal for instructing restart of outputting

the plaintext when the detection signal is outputted.

5. An encryption apparatus for executing an encryption algorithm that receives plaintext to output ciphertext in which the encryption algorithm is changeable, the encryption apparatus comprising:

a receiving part for receiving the plaintext;

a counter part for separating a predetermined part from a bit string forming the plaintext into a fixed part and a remaining part into a variable part, counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of the fixed parts, and storing it as a separate count;

a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number;

an encryption apparatus main body for performing the encryption algorithm for encryption when a detection signal is not outputted from the detecting part, and for holding output of the plaintext when the detection signal is outputted;

an indication signal receiving part for receiving an indication signal for indicating an encryption algorithm for new use; and

a setting part for outputting cipher setting information

required for setting the encryption algorithm executed by the encryption apparatus main body and counter part setting information required for setting information corresponding to the encryption algorithm for the fixed part and the set of the values of the fixed parts and used by the counter part based on the indication signal,

wherein the encryption apparatus main body and the counter part perform the settings based on the cipher setting information and the counter part setting information.

6. An encryption apparatus for executing an encryption algorithm that receives plaintext to calculate ciphertext with a key, the encryption apparatus comprising:

a receiving part for receiving the plaintext;

a counter part for separating a predetermined part from a bit string forming the plaintext into a fixed part and a remaining part into a variable part, counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts formed of 1 or a plurality of the values of the fixed parts at every set of the values of the fixed parts, and storing it as a separate count;

a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number; and

an encryption apparatus main body for updating the key

used for encryption when a detection signal is outputted from the detecting part.

7. A ciphertext storing apparatus for executing an encryption algorithm that receives plaintext to calculate ciphertext with a key, and storing the ciphertext, the ciphertext storing apparatus comprising:

a receiving part for receiving the plaintext;

a counter part for separating a predetermined part from a bit string forming the plaintext into a fixed part and a remaining part into a variable part, counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of the fixed parts, and storing it as a separate count;

a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number;

a ciphertext storing part allowed to store ciphertext; and

a ciphertext storing apparatus main body for updating the key used for encryption when a detection signal is outputted from the detecting part, and for storing partial plaintext being a part of the plaintext, the ciphertext, and key reference information allowing reference of the key having been used for

encryption in the ciphertext storing part.

8. A filter apparatus for limiting output of ciphertext from a block encryption algorithm that receives and stirs plaintext with a key step by step to perform encryption and outputs ciphertext, the filter apparatus comprising:

a receiving part for receiving the plaintext;

a counter part for separating a predetermined part from a bit string forming the plaintext into a fixed part and a remaining part into a variable part, counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of the fixed parts, and storing it as a separate count;

a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number; and

a filter apparatus main body for outputting the plaintext when a detection signal is not outputted from the detecting part, and for holding output of the plaintext until it receives a process restart signal for instructing restart of outputting the plaintext when the detection signal is outputted.

9. An encryption apparatus for executing a block encryption algorithm that receives and stirs plaintext with

a key step by step to perform encryption and outputs ciphertext in which the encryption algorithm is changeable, the encryption apparatus comprising:

a receiving part for receiving the plaintext;

a counter part for separating a predetermined part from a bit string forming the plaintext into a fixed part and a remaining part into a variable part, counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of the fixed parts, and storing it as a separate count;

a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number;

an encryption apparatus main body for executing the encryption algorithm for encryption when a detection signal is not outputted from the detecting part, and for holding output of the plaintext when the detection signal is outputted;

an indication signal receiving part for receiving an indication signal for indicating an encryption algorithm for new use; and

a setting part for outputting cipher setting information required for setting the encryption algorithm executed by the encryption apparatus main body and counter part setting information for setting information corresponding to the

encryption algorithm for the fixed part and the set of the values of the fixed parts and used by the counter part based on the indication signal,

wherein the encryption apparatus main body and the counter part perform the settings based on the cipher setting information and the counter part setting information.

10. An encryption apparatus for executing a block encryption algorithm that receives and stirs plaintext with a key step by step to perform encryption and outputs ciphertext, the encryption apparatus comprising:

a receiving part for receiving the plaintext;

a counter part for separating a predetermined part from a bit string forming the plaintext into a fixed part and a remaining part into a variable part, counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of the fixed parts, and storing it as a separate count;

a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number; and

an encryption apparatus main body for updating the key used for encryption when a detection signal is outputted from the detecting part.

11. A ciphertext storing apparatus for executing a block encryption algorithm that receives and stirs plaintext with a key step by step to perform encryption and outputs ciphertext, and storing the ciphertext, the ciphertext storing apparatus comprising:

a receiving part for receiving the plaintext;

a counter part for separating a predetermined part from a bit string forming the plaintext into a fixed part and a remaining part into a variable part, counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of the fixed parts, and storing it as a separate count;

a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number;

a ciphertext storing part allowed to store ciphertext; and

a ciphertext storing apparatus main body for updating the key used for encryption when a detection signal is outputted from the detecting part, and for storing partial plaintext being a part of the plaintext, the ciphertext, and key reference information allowing reference of the key having been used for encryption in the ciphertext storing part.

12. A filter apparatus for limiting output of ciphertext from a KASUMI type encryption algorithm having a stirring step, the KASUMI type encryption algorithm equal to KASUMI which is a block encryption algorithm that receives plaintext, has a plurality of stirring steps for stir with a key, and performs encryption step by step to output ciphertext, the filter apparatus comprising:

a receiving part for receiving the plaintext;

a counter part for separating 17th to 32nd bits of the plaintext from the plaintext into a fixed part and first to 16th bits and 33rd to 64th bits thereof into a variable part, counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts formed of 1 or a plurality of the values of the fixed parts at every set of the values of the fixed parts, and storing it as a separate count;

a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number; and

a filter apparatus main body for outputting the plaintext when a detection signal is not outputted from the detecting part, and for holding output of the plaintext until it receives a process restart signal for instructing restart of outputting the plaintext when the detection signal is outputted.

13. An encryption apparatus for executing a KASUMI type encryption algorithm having a stirring step, the KASUMI type encryption algorithm equal to KASUMI which is a block encryption algorithm that receives plaintext, has a plurality of stirring steps for stir with a key, and performs encryption step by step to output ciphertext in which the encryption algorithm is changeable, the encryption apparatus comprising:

a receiving part for receiving the plaintext;

a counter part for separating 17th to 32nd bits of the plaintext from the plaintext into a fixed part and first to 16th bits and 33rd to 64th bits thereof into a variable part, counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts formed of 1 or a plurality of the values of the fixed parts at every set of the values of the fixed parts, and storing it as a separate count;

a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number;

an encryption apparatus main body for executing the encryption algorithm for encryption when a detection signal is not outputted from the detecting part, and for holding output of the plaintext when the detection signal is outputted;

an indication signal receiving part for receiving an indication signal for indicating an encryption algorithm for

new use; and

a setting part for outputting cipher setting information required for setting the encryption algorithm executed by the encryption apparatus main body and counter part setting information required for setting information corresponding to the encryption algorithm for the fixed part and the set of the values of the fixed parts and used by the counter part based on the indication signal,

wherein the encryption apparatus main body and the counter part perform the settings based on the cipher setting information and the counter part setting information.

14. An encryption apparatus for executing a KASUMI type encryption algorithm having a stirring step, the KASUMI type encryption algorithm equal to KASUMI which is a block encryption algorithm that receives plaintext, has a plurality of stirring steps for stir with a key, and performs encryption step by step to output ciphertext, the encryption apparatus comprising:

a receiving part for receiving the plaintext;

a counter part for separating 17th to 32nd bits of the plaintext from the plaintext into a fixed part and first to 16th bits and 33rd to 64th bits thereof into a variable part, counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts formed of

1 or a plurality of the values of the fixed parts at every set of the values of the fixed parts, and storing it as a separate count;

a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number; and

an encryption apparatus main body for updating the key used for encryption when a detection signal is outputted from the detecting part.

15. A ciphertext storing apparatus for executing a KASUMI type encryption algorithm having a stirring step, the KASUMI type encryption algorithm equal to KASUMI which is a block encryption algorithm that receives plaintext, has a plurality of stirring steps for stir with a key, and performs encryption step by step to output ciphertext, and storing the ciphertext, the ciphertext storing apparatus comprising:

a receiving part for receiving the plaintext;

a counter part for separating 17th to 32nd bits of the plaintext from the plaintext into a fixed part and first to 16th bits and 33rd to 64th bits thereof into a variable part, counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts formed of 1 or a plurality of the values of the fixed parts at every set of the values of the fixed parts, and storing it as a separate

count;

a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number;

a ciphertext storing part allowed to store ciphertext; and

a ciphertext storing apparatus main body for updating the key used for encryption when a detection signal is outputted from the detecting part, and for storing partial plaintext being a part of the plaintext, the ciphertext, and key reference information allowing reference of the key having been used for encryption in the ciphertext storing part.